



UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/901,176	07/09/2001	Terry L. Cole	2000.053400	6003
23720	7590	07/15/2005	EXAMINER	
WILLIAMS, MORGAN & AMERSON, P.C. 10333 RICHMOND, SUITE 1100 HOUSTON, TX 77042			UNGAR, DANIEL M	
			ART UNIT	PAPER NUMBER
			2132	

DATE MAILED: 07/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/901,176	COLE ET AL.	
	Examiner	Art Unit	
	Daniel M. Ungar	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 27 April 2005.
- 2a) This action is **FINAL**. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-61 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-61 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 27 April 2005 is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) Notice of References Cited (PTO-892)
- 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) Notice of Informal Patent Application (PTO-152)
- 6) Other: _____.

Art Unit: 2132

DETAILED OFFICE ACTION

1. This action is in response to remarks filed 27 April 2005.

DRAWINGS

2. Replacement drawing(s) have been accepted. Objections withdrawn.

OBJECTIONS

3. In response to amendments to claim 15, objection is withdrawn.

REJECTIONS - 35 U.S.C. 112

4. In response to amendments to claims 3, 17, 28, 35, and 47 to correct for indefiniteness, rejections under 35 U.S.C. 112, second paragraph are withdrawn.

RESPONSE TO ARGUMENTS

5. With regard to claims 1-5, 10-12, 49-54, and 56-59, Applicants' arguments have been considered fully but are not found persuasive. Applicants assert that Lazcko et al. fail to teach a secure driver as defined in the specification on page 13. Examiner respectfully disagrees that the referenced specification constitutes a definition. Loading a driver from a secure location may deem the driver secure, but it is not the only way. For example, the secure driver may be stored as a [sic] digitally signed file, as Applicants point out. Thus Lazcko et al., whose processor processes encryption and digital signatures (see column 6, lines 37-67), and verification program code stored with a digital signature (see column 5, lines 6-17), disclose a driver that is indeed secure.

6. With regard to claims 15-19, 23, 25, 26-30, 34, 36, 37-41, 46, and 48, Applicants' arguments have been considered fully but are not found persuasive. Applicants assert that because in Bialick et al. the host automatically provides the user with the opportunity to instruct the host to transfer the peripheral device driver, that driver is not deemed secure. Examiner respectfully disagrees. Although Applicants do not specify clearly where in Bialick et al. this assertion comes from, the fact that the functionality from the peripheral device is automatic

does not detract from the fact that "the security operations are performed between communication of data to or from the host computing device" (see abstract). As limited by the instant claims, Bialick et al. still describe a secure driver.

7. Similarly regarding the arguments to the rejections under 35 U.S.C. 103(a) for claims 6-9, 13-14, 20-22, 31-33, 42-45, 55, and 60-61, Examiner asserts that the drivers disclosed by both Lazcko et al. and Bialick et al. do not lack the security necessary to prevent them from being described as "secure drivers" with respect to the limitations found in independent claims 1, 15, and 49.

CLAIM REJECTIONS – 35 U.S.C. 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

- (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.
- (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

9. The following claims are rejected under 35 U.S.C. 102(e) as being anticipated by Laczko et al., U.S. Patent Number 6,775,778: Claims 1-5, 10-12, 49-54, and 56-59.

10. Regarding claim 1, Laczko et al. disclose a communications system comprising: physical layer hardware adapted to communicate data over a communications channel, to demodulate an incoming analog signal to generate a digital receive signal and modulate a digital transmit signal to generate an analog transmit signal (see column 3, line 52 – column 4, line 4); and

a processing unit adapted to load a secure driver for interfacing with the physical layer hardware, the secure driver including program instructions for implementing a protocol layer to decode the digital receive signal and encode the digital transmit signal (see column 4, lines 19-43). Note that "driver" has a definition, "a program, circuit, or device used to power or control other programs, circuits, or devices" (The Authoritative Dictionary of IEEE Standards Terms, 7th Edition). Accordingly, the "central processing unit" of Laczko et al. which includes "digital signal processing capability" (see column 4, lines 25-37), and a real time operating system "enabling digital media processor to receive and process various data streams" (see column 5, lines 30-40) meets the limitation of the processing unit of this claim.

11. Regarding claim 2, Laczko et al. disclose a digitally signed file (see column 5, lines 8-16).
12. Regarding claim 3, Laczko et al. disclose memory containing the real time operating system and its corresponding signature portion (see column 5, lines 22-50), meeting the limitation of a secure program storage device adapted to store the secure modem driver.
13. Regarding claim 4, Laczko et al. disclose flash memory (see column 5, lines 22-50).
14. Regarding claim 5, Laczko et al. disclose a processing unit comprising a computer (title, abstract, column 2, lines 19-33).
15. Regarding claim 10, Laczko et al. disclose a program storage device to store a public key for authenticating the digitally signed file (see column 5, lines 22-50).
16. Regarding claim 11, Laczko et al. disclose Boot ROM which includes public signature keys (see column 4, line 61 – column 5, line 17). Note that BIOS is defined as the "essential software routines that tests hardware at startup, [and] starts the operating system" (Microsoft Computer Dictionary, 5th Edition). The Boot ROM disclosed meets the limitation of BIOS as claimed.

17. Regarding claims 12, Laczko et al. disclose securing the device by an authentication key (see column 5, lines 8-16).
18. Regarding claim 49, Laczko et al. disclose a method for providing a secure driver, comprising storing and loading a secure driver, including program instructions for implementing a communication protocol, and communicating data over a communications channel based on the program instructions in the secure driver (see abstract; column 2, lines 18-22; column 4, lines 19-43; column 7, line 12-13). Note that "driver" has a definition, "a program, circuit, or device used to power or control other programs, circuits, or devices" (The Authoritative Dictionary of IEEE Standards Terms, 7th Edition). Accordingly, the "central processing unit" of Laczko et al. which includes "digital signal processing capability" (see column 4, lines 25-37), and a real time operating system "enabling digital media processor to receive and process various data streams" (see column 5, lines 30-40) meets the limitation of the processing unit of this claim.
19. Regarding claim 50, Laczko et al. disclose demodulating an incoming analog signal to generate a digital receive signal and modulating a digital transmit signal to generate an analog transmit signal (see column 3, line 52 – column 4, line 4); and decoding the digital receive signal based on the program instructions in the secure driver and encoding the digital transmit signal based on the program instructions in the secure driver (see column 4, lines 19-43).
20. Regarding claim 51, Laczko et al. disclose a digitally signed file (see column 5, lines 8-16).
21. Regarding claim 52, Laczko et al. disclose memory containing the real time operating system and its corresponding signature portion (see column 5, lines 22-50), meeting the limitation of a secure program storage device adapted to store the secure modem driver.
22. Regarding claim 53, Laczko et al. disclose flash memory (see column 5, lines 22-50).

23. Regarding claim 54, Laczko et al. disclose a processing unit comprising a computer (title, abstract, column 2, lines 19-33).
24. Regarding claim 56, Laczko et al. disclose Boot ROM memory adapted to store the secure driver (see column 2, lines 18-33). Note that BIOS is defined as the “essential software routines that tests hardware at startup, [and] starts the operating system” (Microsoft Computer Dictionary, 5th Edition). The Boot ROM disclosed meets the limitation of BIOS as claimed. Note that the real time operating system disclosed meets the limitation of driver as claimed, as noted above.
25. Regarding claim 57, Laczko et al. disclose a program storage device to store a public key for authenticating the digitally signed file (see column 5, lines 22-50).
26. Regarding claim 58, Laczko et al. disclose Boot ROM which includes public signature keys (see column 4, line 61 – column 5, line 17). Note that BIOS is defined as the “essential software routines that tests hardware at startup, [and] starts the operating system” (Microsoft Computer Dictionary, 5th Edition). The Boot ROM disclosed meets the limitation of BIOS as claimed.
27. Regarding claims 59, Laczko et al. disclose securing the device by an authentication key (see column 5, lines 8-16).
28. **The following claims are rejected under 35 U.S.C. 102(a) as being anticipated by Bialick et al., U.S. Patent Number 6,088,802: Claims 15-19, 23, and 25; 26-30, 34, and 36; 37-41, 46, and 48.**
29. Regarding claim 15, Bialick et al. disclose a computer system comprising a processor complex adapted to load a secure driver including program instructions for implementing a communications protocol (see abstract; column 6, lines 28-33; column 5, lines 10-18); a bus

coupled to the processor complex (see column 6, lines 28-45); and an expansion card coupled to the bus (see column 6, line 65 – column 7, line 2) including physical layer hardware adapted to communicate data over a communications channel as a modem (see column 13, lines 50-62). Note that a modem is defined to be a device that modulates digital signals to analog signals and demodulates analog signals to digital signals (The Authoritative Dictionary of IEEE Standard Terms, 7th Edition), and thus it meets the limitations in this claim.

30. Regarding claim 16, Bialick et al. disclose the secure driver comprising a digitally signed file (see column 16, lines 57-67; column 18, lines 12-16).

31. Regarding claim 17, Bialick et al. disclose a secure program storage device to store the secure driver (column 9, lines 5-25).

32. Regarding claim 18, Bialick et al. disclose secure program storage device comprising a flash memory (column 13, lines 27-36).

33. Regarding claim 19, Bialick et al. disclose the secure program storage device located on the expansion card (see column 7, line 60 – column 8, line 14).

34. Regarding claim 23 and 25, Bialick et al. disclose securing the program storage device by an authentication key, and a password (see column 10, line 45-61).

35. Regarding claim 26, Bialick et al. disclose a computer system comprising a peripheral device (see title, abstract, column 1, lines 16-27) and a processor complex coupled to the peripheral device (see column 6, lines 28-33) and adapted to load a secure driver including program instructions for interfacing with the peripheral device (see column 5, lines 10-18; column 6, lines 28-33; column 8, lines 50-61).

36. Regarding claim 27, Bialick et al. disclose the secure driver comprising a digitally signed file (see column 16, lines 57-67; column 18, lines 12-16).

37. Regarding claim 28, Bialick et al. disclose a secure program storage device to store the secure driver (column 9, lines 5-25).
38. Regarding claim 29, Bialick et al. disclose secure program storage device comprising a flash memory (column 13, lines 27-36).
39. Regarding claim 30, Bialick et al. disclose secure program storage device located on the peripheral device (column 9, lines 18-22).
40. Regarding claims 34 and 36, Bialick et al. disclose securing the program storage device by an authentication key, and a password (see column 10, line 45-61).
41. Regarding claim 37, Bialick et al. disclose a method for protecting a software driver comprising storing a secure driver in a computer system, the secure driver program including program instructions for interfacing with a peripheral device (see column 5, lines 10-18), loading the secure driver and interfacing the peripheral device using the secure driver (see column 7, lines 17-25).
42. Regarding claim 38, Bialick et al. disclose the secure driver comprising a digitally signed file (see column 16, lines 57-67; column 18, lines 12-16).
43. Regarding claim 39, Bialick et al. disclose a secure program storage device to store the secure driver (column 9, lines 5-25).
44. Regarding claim 40, Bialick et al. disclose storing the secure driver in flash memory (column 13, lines 27-36).
45. Regarding claim 41, Bialick et al. disclose secure program storage device located on the peripheral device (column 9, lines 18-22).

46. Regarding claims 46 and 48, Bialick et al. disclose securing the program storage device by an authentication key, and a password (see column 10, line 45-61).

CLAIM REJECTIONS - 35 U.S.C. 103(a)

47. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

48. The following claims are rejected under 35 U.S.C. 103(a) as being unpatentable over Laczko et al. in view of Bialick et al: Claims 6-9, 14, 55, and 61.

49. Regarding claim 6, Laczko et al. disclose a processor complex adapted to execute the program instructions in the secure driver (see column 4, lines 19-43). However, Laczko et al. does not specify the manner by which the physical layer hardware is coupled to the processor complex. Specifically, Laczko et al. do not disclose an expansion card coupled to a bus. Nevertheless, Bialick et al., in a similar field of endeavor, disclose a peripheral expansion card coupled to a bus which is coupled to a processor complex (see column 5, lines 40-49; column 6, lines 19-51). The card includes physical layer hardware (see column 5, lines 10-18). It would have been obvious to one of ordinary skill in the art at the time of the invention to have utilized the expansion card method of processor-peripheral coupling as disclosed by Bialick et al. in the system of Laczko et al. to achieve more modularity in coupling the physical layer hardware to the processor complex.

50. As for claims 7 and 8, Bialick et al. disclose the secure program storage device is located on either the expansion card, or in the computer (see column 9, lines 5-9 and 14-20). It would have been obvious to one of ordinary skill in the art to allow the computer of Laczko et al. to

access program storage on the peripheral device (expansion card) in order for the driver to be close to the physical layer hardware or on the computer to store the driver in order for the driver to be close to the processor complex.

51. Regarding claim 9, Laczko et al. disclose Boot ROM memory adapted to store the secure driver (see column 2, lines 18-33). Note that BIOS is defined as the “essential software routines that tests hardware at startup, [and] starts the operating system” (Microsoft Computer Dictionary, 5th Edition). The Boot ROM disclosed meets the limitation of BIOS as claimed. Note that the real time operating system disclosed meets the limitation of driver as claimed, as noted above.

52. Regarding claim 14, Laczko et al. fails to disclose securing the program storage device by a password. However, restricting access to program storage devices based on a password was well known in the art at the time of the invention. For example, Bialick et al. discloses in a similar field of endeavor, securing a peripheral device driver by a password (see column 10, lines 45-47; column 11, lines 8-11). It would have been an obvious modification to one of ordinary skill in the art at the time of the invention to the system of Laczko et al. to require a password to gain access to the driver on the program storage device. This would authenticate the user, or identify the user, as disclosed by Bialick et al.

53. Regarding claim 55, Laczko et al. disclose a processor complex adapted to execute the program instructions in the secure driver (see column 4, lines 19-43). However, Laczko et al. does not specify the manner by which the physical layer hardware is coupled to the processor complex. Specifically, Laczko et al. do not disclose an expansion card coupled to a bus. Nevertheless, Bialick et al., in a similar field of endeavor, disclose a peripheral expansion card coupled to a bus which is coupled to a processor complex (see column 5, lines 40-49; column 6, lines 19-51). The card includes physical layer hardware (see column 5, lines 10-18). It would have been obvious to one of ordinary skill in the art at the time of the invention to have utilized the expansion card method of processor-peripheral coupling as disclosed by Bialick et al. in the

system of Laczko et al. to achieve more modularity in coupling the physical layer hardware to the processor complex.

54. Regarding claim 61, Laczko et al. fails to disclose securing the program storage device by a password. However, restricting access to program storage devices based on a password was well known in the art at the time of the invention. For example, Bialick et al. discloses in a similar field of endeavor, securing a peripheral device driver by a password (see column 10, lines 45-47; column 11, lines 8-11). It would have been an obvious modification to one of ordinary skill in the art at the time of the invention to the system of Laczko et al. to require a password to gain access to the driver on the program storage device. This would authenticate the user, or identify the user, as disclosed by Bialick et al.

55. **The following claims are rejected under 35 U.S.C. 103(a) as being unpatentable over Laczko et al. in view of Novoa, et al., U.S. Patent Number 6,223,284: Claims 13, 14, 60, and 61.**

56. Regarding claims 13 and 60, Although Laczko et al. disclose securing the physical layer hardware with an authentication key, they do not explicitly disclose receiving the key over the communications channel. However, receiving authentication keys over communications channels was well known in the art at the time of the invention. For example, Novoa et al. disclose the remote update of the flash ROM in a computer system using digital signatures in which the public key is received remotely over a communications channel (see column 10, line 30-45; column 20, lines 33-60; column 21, lines 49-58). Novoa et al. also disclose receiving a password, which is also an authentication key, over a communications channel (see abstract). It would have been obvious to one of ordinary skill in the art at the time of the invention to have modified the system of Laczko et al. to allow for the key to be received over the communications channel so that it could be accessed remotely.

57. Regarding claims 14 and 61, Laczko et al. fail to disclose securing the program storage device with a password. However, the use of a password to restrict access to a program storage

device was well known in the art at the time of the invention. Exemplary of this is Novoa et al. who, in a similar field of endeavor, disclose securing the secure program storage device with a password (abstract). It would have been obvious to one of ordinary skill in the art at the time of the invention to have modified the system of Laczko et al. to require a password as per Novoa et al. to further secure access to the program storage device.

58. The following claims are rejected under 35 U.S.C. 103(a) as being unpatentable over Bialick et al. in view of Laczko et al.: Claims 20-22, 31-33, and 42-45.

59. Regarding claims 20-22 and 31-33, and 42-45, although Bialick et al. disclose storing the driver and the public key on memory of the computer system, they do not explicitly disclose storing the driver or the public key in the BIOS memory of the computer system, and using it to authenticate the digitally signed file. Nevertheless, Laczko et al. in a similar field of endeavor disclose Boot ROM memory adapted to store the secure driver (see column 2, lines 18-33). Specifically regarding claims 21, 32, and 43, Laczko et al. also disclose an associated program storage device to store a public key for authenticating the digitally signed file (see column 5, lines 22-50). Specifically regarding claim 45, Laczko et al. disclose loading the secure driver during an initialization of the computer system (see column 2, lines 18-33; column 4, line 61 - column 5, line 17; figure 5). Note that BIOS is defined as the "essential software routines that tests hardware at startup, [and] starts the operating system" (Microsoft Computer Dictionary, 5th Edition). The Boot ROM disclosed meets the limitation of BIOS as claimed. Note that "driver" has a definition, "a program, circuit, or device used to power or control other programs, circuits, or devices" (The Authoritative Dictionary of IEEE Standards Terms, 7th Edition). Accordingly, the "central processing unit" of Laczko et al. which includes "digital signal processing capability" (see column 4, lines 25-37), and a real time operating system "enabling digital media processor to receive and process various data streams" (see column 5, lines 30-40) meets the limitation of the processing unit of this claim. It would have been an obvious modification to one of ordinary skill in the art at the time of the invention to the method of Bialick et al. to store the driver and the public key for authenticating the digitally

signed file in the BIOS to make them inaccessible from outside the system, as explained by Laczko et al. (see column 2, lines 23-24), thus providing security.

60. The following claims are rejected under 35 U.S.C. 103(a) as being unpatentable over Bialick et al. in view of Novoa et al., U.S. Patent Number 6,223,284: Claims 24, 35, and 47.

61. Regarding claims 24, 35, and 47, as best understood, although Bialick et al. disclose securing the physical layer hardware with an authentication key, they do not explicitly disclose receiving the key over the communications channel. However, receiving authentication keys over communications channels was well known in the art at the time of the invention. For example, Novoa et al. disclose the remote update of the flash ROM in a computer system using digital signatures in which the public key is received remotely over a communications channel (see column 10, line 30-45; column 20, lines 33-60; column 21, lines 49-58). Novoa et al. also disclose receiving a password, which is also an authentication key, over a communications channel (see abstract). It would have been obvious to one of ordinary skill in the art at the time of the invention to have modified the system of Bialick et al. to allow for the key to be received over the communications channel so that it could be accessed remotely.

CONCLUSION

62. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel M. Ungar whose telephone number is 571.272.7960. The examiner can normally be reached on 8:30 - 6:00 Monday - Thursday, Alt. Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571.272.3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2132

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Art Unit 2132

DMU
Daniel M. Ungar.

Gilberto Barron Jr.
GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100